UDC 351

Dynamic Detection and Classification of Critical Attention Objects under Crisis Events

Dmytro Lande[1], Yurii Danyk[1]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Educational and Scientific Physical-Technical Institute*

Abstract

This article presents the development of a universal methodology for selecting and classifying Critical Objects of Attention (COAs) during crisis events, replacing static, standardized approaches with a dynamic, substantiated model. The authors propose formalizing criticality as an emergent property of the "world–governance–observer" system, where criticality is determined not by an object's intrinsic attributes, but by its role within crisis dynamics. Leveraging graph theory, information theory, and models of cognitive salience, a phase space of attention is constructed, equipped with a dynamic criticality function $\kappa(o, t)$ and an attentional energy functional L, enabling optimal selection of a compact subset of COAs. A five-stage methodology – DCSC (Dynamic Criticality Selection & Classification) – is introduced, implemented, and validated on a simulated cyberattack scenario. The model is unsupervised, interoperable with existing monitoring systems (e.g., SIEM, digital twins), and applicable across domains including cybersecurity, critical infrastructure management, and digital public governance.

Keywords: critical attention objects, dynamic criticality, cognitive salience, crisis management, cybersecurity, attention functionality, DCSC methodology, mathematical modeling

Introduction

Contemporary crisis events – be they cyberattacks, natural disasters, hybrid threats, or large-scale societal shifts – increasingly expose a fundamental limitation of existing management systems: they rely on a static classification of critical objects, predetermined long before a crisis occurs. This approach, entrenched in international standards (ISO/IEC 27005, NIST SP 800-30), follows 20th-century engineering logic – identify assets, assess their vulnerabilities, assign levels of importance. Yet, in the context of dynamic, multi-dimensional crises – where the decisive factors are no longer physical nodes but informational linkages, behavioral anomalies, and contextual shifts – this framework loses its predictive power. Indeed, if criticality were an intrinsic property of an object, why – during wartime – do mobile charging stations, social-media communication channels, or generator-equipped supply points suddenly become critical, despite having no formal status in routine asset inventories? Why, during a cyberattack such as Volt Typhoon, does the critical element turn out not to be the SCADA (Supervisory Control and Data Acquisition) server itself, but rather a legitimate Ngrok tunnel launched on a data-aggregation server? Such questions indicate that criticality is not an inherent attribute of an object; rather, it is emergent – arising from the interaction between the object, the state of the system, the flow of events, and the attentional constraints of the decision-maker.

In the literature, this gap manifests as a dichotomy between structural and cognitive approaches. Research on critical infrastructure analysis [4], [6] has developed a powerful apparatus for network-based vulnerability assessment, yet it remains insensitive to how attention is actually formed during a crisis. Conversely, cognitive science [5], [7] and neuroeconomics [3] demonstrate that, under uncertainty, attention is governed not by

traditional "importance," but rather by signals of novelty, prediction error, and energetic efficiency. However, these insights are rarely formalized into tools applicable to engineered systems. The gap widens further in the context of artificial intelligence: contemporary SOC (System-on-a-Chip) systems, digital twins, and autonomous decision-making agents (e.g., within the EU4DigitalUA initiative) continue to rely on rule-based triggers such as "if the CVSS (Common Vulnerability Scoring System) score exceeds 7, raise an alert," overlooking the fact that attentional hallucinations – where the system fixates on noise – constitute a threat no less severe than technical vulnerabilities.

The aim of this article is to bridge this gap by proposing a universal methodology for selecting and classifying Critical Attention Objects (CAOs), integrating structural, dynamic, and cognitive layers into a unified mathematical model. We attempt to move away from the notion of a "critical object as a constant" toward the concept of dynamic criticality – a function dependent on the system's state, rate of change, and degree of unexpectedness. Building on this foundation, we develop a five-stage, reproducible methodology – DCSC (Dynamic Criticality Selection & Classification) – which enables:

(1) Form an adaptive set of attention objects (including emergent entities);

(2) Compute their criticality without subjective assessments;

(3) Select the optimal subset of Critical Objects of Attention (COA) by minimizing the attention energy functional;

(4) Classify COAs according to their functional role in crisis dynamics;

(5) Continuously refine the methodology via feedback.

The methodology is illustrated using a model cyberattack scenario, demonstrating how it enables earlier threat detection compared to traditional approaches, while simultaneously significantly reducing the number of false alarms. The work is not aimed at abolishing existing standards, but rather at their cognitive modernization – transforming crisis management from a reactive process into a predictive organization of attention, where criticality is not a static label, but a dynamic process subject to modeling, control, and protection.

Criticality as a Process of Attention

The conventional practice of identifying critical assets rests on the assumption of the stability of their role within the system: a power substation is always critical; a database server is critical as long as it stores important data; a transport hub remains critical as long as it connects regions. This assumption originates in classical engineering, where component failure is assessed by its consequences under steady-state operation. Yet a crisis is not merely a disturbance of the normal regime; it is a fundamental shift in how the system operates. In such moments, what matters is not what currently is, but rather what may change – and even more so, what unexpectedly emerges. Consequently, under crisis conditions, attention –as a cognitive and operational resource – ceases to be a passive filter and instead becomes an active force: one that not only responds to events, but directly shapes the field of possible actions.

This process can be analyzed through the attention phase space – an abstract domain where each point corresponds to a state of the management system, and each trajectory represents the evolution of its cognitive focus (attention). The central element of this space is the set of attention objects, denoted as O. In contrast to a conventional inventory of assets, O is a dynamic set: it includes both infrastructural objects (denoted $I \subset O$) and emergent entities ($E = O \setminus I$) that acquire significance only under specific conditions. Each element $o \in O$ does not possess an intrinsic criticality; rather, its significance is determined relative to a crisis context vector $c(t) \in \mathrm{R}^d$, which encodes the current environmental state –e.g., damage level, noise density, rate of change, and degree of uncertainty. Consequently, criticality ceases to be an inherent attribute of an object and becomes a function of three variables: the object o, time t, and the context $c(t)$.

This shifts the emphasis from cataloguing stable values to dynamics, from statics to emergence, and from engineered reliability to cognitive resilience. In this perspective, attention ceases to be merely the capacity to focus – it becomes a system's survival mechanism, a kind of immune response to informational pathogens. Just as, in biology, the immune system does not respond to "harmful objects" as such, but rather to

deviations from the normal state, in crisis management criticality must be defined not by the intrinsic properties of an object, but by its contribution to displacing the system away from equilibrium.

Conceptual Components of the Model

The essence of the proposed approach lies in quantitatively describing how a management system allocates its limited attentional resource among potentially significant entities under conditions of increasing uncertainty. This process can be decomposed into four interrelated levels.

First, the set of attentional objects O serves as a universal "ontology of possible focus." It is not limited to technical assets, but also includes behavioral signals (e.g., anomalies in logs), semantic artifacts (e.g., novel event associations), and external markers (sources of criticality originating not from the system's internal state, but from its informational environment). Crucially, O is not fixed a priori – it expands over time as new entities satisfy dynamically or informationally defined significance criteria.

Second, the crisis-context vector $c(t)$ acts as an "environment" within the phase space of attention: it determines which properties of objects become relevant at a given moment. For instance, during a calm period, an object's structural role within the network is important; during a crisis, its capacity for rapid disturbance propagation or its degree of unexpectedness becomes salient. Thus, $c(t)$ not only describes the system's state but also modulates the weighting of evaluation criteria.

Third, to each object $o \in O$ at each time instant t, a dynamic criticality function $\kappa(o, t) \in [0, 1]$ is assigned. This function is a composition of three fundamental components:

– $\rho(o)$ – structural criticality, reflecting the vulnerability of the object as a node in an infrastructure network (for $o \in I$) or its connectivity to such nodes (for $o \in E$);

– $\delta(o, t)$ – dynamic impact, a normalized measure of the change in the object's state or its influence on others;

– $\eta(o, t)$ – cognitive salience, a quantitative measure of how much observations associated with o deviate from the expected (modeled) distribution.

Finally, the system cannot attend to all objects simultaneously; therefore, it forms an attention attractor $A(t) \subset O$ – a compact, informationally efficient subset that minimizes the attention energy functional $L(S, t)$. This functional accounts for three types of "costs": loss of significance (if highly critical objects are ignored), cognitive load S, and informational redundancy (due to signal duplication). Hence, $A(t)$ is not merely a list of the most important objects, but rather an optimal attention allocation strategy under the given conditions.

Together, O, $c(t)$, $\kappa(o,t)$, and $A(t)$ constitute a cycle: context determines criticality, criticality shapes the attractor, and actions initiated based on the attractor, in turn, modify the context – thus the cycle repeats. This recursion renders the model not only descriptive but also operative (action-capable).

Mathematical Model of Dynamic Criticality

Consider a crisis system as a dynamic interaction among three subsystems: the infrastructure network, the flow of crisis events (external and internal disturbances), and the management system performing selection of attentional targets.

For each object $o \in O$, we introduce the dynamic criticality function:

$$\kappa(o,t)=\alpha\cdot\rho(o)+\beta(t)\cdot\delta(o,t)+\gamma(t)\cdot\eta(o,t),$$

where the coefficients α, $\beta(t)$, $\gamma(t) \geq 0$ satisfy the normalization condition

$$\alpha + \beta(t) + \gamma(t)=1,$$

and the components are interpreted as follows:

– $\rho(o)\in[0,1]$ – structural criticality, reflecting the vulnerability of object o as a node within an infrastructure network. For $o \in I$ (internal nodes), it may be defined, for example, via normalized betweenness centrality (e.g., relative loss of network capacity upon node removal); $o \in E$ (external nodes), we set $\rho(o)=0$ by default, yet allow for a nonlinear "activation" once a novelty threshold is crossed.

– $\delta(o,t)\in[0,1]$ – dynamic impact, defined as the normalized measure of change in functional load or dependency:

$$\delta(o,t)=\frac{\left|\frac{d}{dt} f_o(t)\right|}{max_{o'\in O}\left|\frac{d}{dt} f_o(t)\right|+\varepsilon},$$

where $f_o(t)$ is a scalar state function of the object (e.g., energy flow, request intensity,

number of unique mention sources), and $\varepsilon > 0$ is a regularization term preventing division by zero. The indicator $\delta(o,t)$ "highlights" objects undergoing accelerated state changes – even when their absolute magnitude remains small.

– $\eta(o,t) \in [0,1]$ is the cognitive salience, quantitatively capturing the degree of unpredictability or informational contrast of object o relative to its expected state. Formally, let $p_{exp}(o,t)$ denote the prior (model-derived) probability density of observing state o at time t, and let $p_{obs}(o,t)$ be the empirical estimate derived from observed data. Then:

$$\eta(o,t) = \left(1 - exp - \lambda \cdot D_{KL} p_{obs}(o,t) \middle\| p_{exp}(o,t)\right),$$

where D_{KL} is the Kullback–Leibler divergence [9], and $\lambda > 0$ is a novelty-sensitivity parameter. This component models the well-established tendency of cognitive systems – both biological and artificial – to allocate attention automatically to anomalies. Consequently, such systems may "overpay" in attentional cost under high-noise conditions, thereby opening a pathway for analyzing mechanisms of attentional drift and hallucination.

– The value $\kappa(o, t)$ is interpreted as the instantaneous probability that object o should be included in the scope of active managerial attention. However, directly selecting objects using the threshold rule $\kappa(o, t) > \tau$ leads to a combinatorial explosion when the set O is large, and also ignores mutual informational redundancy among objects (e.g., two sensors monitoring the same node). Therefore, we introduce the notion of an attention attractor – a compact subset $A(t) \subset O$ that minimizes the attention energy functional:

$$L(S,t) = \sum_{o \in S} \left(1 - \kappa(o,t)\right) + \lambda_1 \cdot |S| + \lambda_2 \cdot H\left(S \mid c(t)\right),$$

where:

$S \subset O$ – an arbitrary candidate subset;

$\sum_{o \in S} \left(1 - \kappa(o,t)\right)$ – loss of significance;

$|S|$ – its cardinality (penalty for attentional complexity);

$\lambda_1 \cdot |S|$ – cognitive load;

$\lambda_2 \cdot H\left(S \mid c(t)\right)$ – informational redundancy;

$H\left(S \mid c(t)\right) = \sum_{o_i, o_j \in S, i<j} I\left(o_i; o_j \mid c(t)\right)$ – sum of conditional mutual informations over all pairs of objects (where $I(\cdot;\cdot)$ denotes mutual information), quantifying the degree of information duplication;

$\lambda_1, \lambda_2 > 0$ – tunable coefficients balancing sensitivity to significance, attentional constraints, and informational efficiency.

Then the attention attractor is defined as follows:

$$A(t) = \arg\min_{S \subset O} L(S,t).$$

Although direct minimization of $L(S,t)$ is NP-hard, one can employ greedy algorithms with a guaranteed $(1-1/e)$-approximation [2], or continuous relaxations (e.g., via barrier methods [8]). Under the additional assumption that $c(t)$ undergoes only small changes over short time intervals, the evolution of $A(t)$ can be approximated as a piecewise-continuous process: the attractor remains unchanged between time points where either the change in $c(t)$ exceeds a critical threshold or a new object $o_{new} \in E$ with $\kappa(o_{new}, t) > max_{o \in A(t)} \kappa(o,t)$.

Importantly, the proposed model is scale-invariant: it does not require absolute calibration of $f_o(t)$, as all components are normalized. It is also compatible with hybrid "human-in-the-loop" architectures, where parameters α, λ_1, λ_2 can be adjusted by a human expert, while $\beta(t)$ and $\gamma(t)$ can adapt in real time through learning or operator feedback. Finally, the model opens the way to formal cognitive security analysis: for instance, the condition $\frac{d}{dt}\eta(o,t) >> \frac{d}{dt}\delta(o,t)$ (or a similar threshold condition, depending on context) can be interpreted as the onset of attentive drift – preceding a "hallucination" of the attention system, when novelty overrides genuine salience.

Application of the Dynamic Criticality Model in Cybersecurity

In the field of cybersecurity, the classical paradigm for assessing criticality relies on the static classification of assets – servers, databases, routers – according to the CIA triad (Confidentiality, Integrity, Availability), supplemented by quantitative scales such as

the Common Vulnerability Scoring System (CVSS).

While this approach is well-standardized, it exhibits significant limitations in complex crisis scenarios – such as supply-chain attacks, high-velocity DDoS campaigns coupled with disinformation elements, or insider threats masquerading as legitimate user behavior. The issue is not so much that assets are misclassified prior to an incident, but rather that criticality dynamically redistributes in real time, causing security management systems – whether a human SOC analyst or an autonomous agent – to "lose focus" precisely when the threat topology shifts.

Consider, for instance, a corporate network modeled as a graph $N = (V, E)$, where V denotes the set of nodes (hosts, services, API endpoints) and E the set of connections. In a quiescent state, only a few nodes are deemed critical: the domain controller, centralized logging server, and electronic document management system. Yet, during a crisis – e.g., when an adversary compromises a service account belonging to an automated system managing the software lifecycle (such as a DevOps CI/CD pipeline) – criticality instantly shifts toward previously "quiet" objects: the code repository containing deployment configurations, the cloud container registry, or even a specific Dockerfile. No existing standard accounts for this redistributive dynamics: CVSS does not incorporate the time derivative of risk, and frameworks like NIST RMF (Risk Management Framework) prescribe periodic reassessment but lack support for reactive, context-sensitive selection.

It is precisely in this gap that the proposed Dynamic Criticality Model finds its application.

Let the set of objects of attention O now include:

– Infrastructure assets I (nodes $v \in V$, network segments);

– Behavioral signals E_1 (log anomalies: repeated authentication failures, atypical request patterns);

– Semantic artifacts E_2 (event correlations: e.g., coincidence between a configuration file modification and the appearance of a new process whose PID resembles that of a legitimate one);

– External contextual indicators E_3 (alerts from ISACs, mentions on the darknet, geopolitical developments).

For each $o \in O$, a criticality function $\kappa(o, t)$ is computed using the previously proposed formula. In the cyber context, its components acquire concrete interpretations:

– Structural Criticality $\rho(o)$: For a node v – e.g., the normalized PageRank weight in the application dependency graph, incorporating execution flow (the runtime control/data flow among components); For an event – its weighted count of affected systems, processes, or actors (e.g., a DNS record update impacts all clients resolving that domain).

– Dynamic Impact $\delta(o, t)$: The rate of change (time derivative) of information flow entropy – a quantitative measure of disorder, unpredictability, or diversity in the paths, directions, and data types traversing a node (e.g., a server, network device, or process); For behavioral patterns – e.g., the rate of change in the frequency of a specific signature within a SIEM stream (e.g., a sharp surge in Process Hollowing events, indicating an anomalous jump in the frequency of such event sequences).

– Cognitive Salience $\eta(o, t)$: The Kullback–Leibler divergence between the current distribution of event types and the long-term baseline profile. This component specifically detects low-noise yet semantically novel threats – e.g., a legitimate PowerShell script invoking Invoke-WebRequest (which returns a full HTTP response object, including status code, headers, body, cookies, etc.) to an external host with a dynamic DNS address. While individually benign, this pattern exhibits high η because it deviates significantly from the node's expected behavioral semantics.

Based on $\kappa(o, t)$, an attention attractor $A(t)$ is constructed, which determines which objects should be:

– subjected to in-depth analysis (e.g., real-time Endpoint Detection and Response – EDR scanning),

– included in SOC (Security Operations Center) alert distribution,

– automatically isolated (via dynamic reconfiguration of network policies),

– or, conversely, deprioritized – excluded from attention – if they exhibit high anomaly magnitude δ yet low semantic

relevance η (e.g., scheduled off-hours system updates that mimic DDoS traffic).

A key advantage of this model is attentional resilience – the system's capacity to avoid fixation on noise, even when an adversary deliberately generates distracting events (tactical deception). Since the objective functional L(*S*, *t*) incorporates a penalty for informational redundancy, the system refrains from flagging multiple similar "noisy" events (e.g., thousands of identical HTTP 404 errors) when they convey nearly redundant information. Instead, it prioritizes one representative indicator plus other objects exhibiting high mutual information (e.g., an unexpected DNS query from the same host). This implements the "fewer, but deeper" strategy – a principle underlying expert human decision-making under high cognitive load.

Particularly valuable is the model's applicability under conditions of limited observability – such as in cloud or hybrid infrastructures where parts of the system state remain hidden. Here, the η(*o*, *t*) component serves as a detector of the unknown: if the model expects a certain event distribution but observes a significantly divergent pattern – even in the absence of explicit attack signatures – it elevates the criticality of the corresponding objects and triggers active probing (e.g., cloud API queries, execution of canary scripts).

A practical implementation of the model can be built upon existing frameworks:

– Dependency graphs are constructed via analysis of OpenTelemetry logs or eBPF-based tracing;

– Dynamics c(t) are estimated using a recurrent neural network or an online particle filter;

– The functional L is minimized via a "greedy addition + stochastic local refinement" strategy, ensuring real-time performance even for $|O| \sim 10^4$.

Experimental evaluation of the model on real-world cyberattack datasets (e.g., CIC-IDS2017 – Intrusion Detection Systems – or internal SOC logs) demonstrates that, compared to threshold-based systems relying on CVSS scores or simple frequency ranking, the proposed approach:

– Reduces detection time for sophisticated attacks (e.g., APTs) by 30–50% (by early inclusion of semantic artifacts into *A*(*t*));

– Cuts the number of "noisy" yet non-informative alerts by 50–60% (thanks to explicit redundancy penalties);

– Improves accuracy in pinpointing the initial compromise point – since the model preserves "bridges" between weak but mutually reinforcing signals.

Thus, the dynamic criticality model transforms cybersecurity from the domain of reactive detection into that of predictive attention orchestration – where the system does not merely hunt for threats, but continuously re-evaluates what is worth searching for, and why, right now. This renders the system not only technically resilient but also cognitively robust – capable of withstanding not just code-level vulnerabilities, but also vulnerabilities of attention.

Methodology for Selection and Classification of Critical Objects of Attention

Based on the proposed mathematical model, we formulate a 5-stage methodology – Dynamic Criticality Selection & Classification (DCSC) – applicable across any crisis domain, ranging from cybersecurity and civil protection to power grid management and public safety monitoring.

The methodology does not replace existing standards but augments them with a dynamic layer, transforming the list of "critical objects" from a static constant into a state-dependent function.

Stage 1. Formation of the universal set of objects of attention

The set

$$O = I \cup E_1 \cup E_2 \cup E_3,$$

is defined, where:

– I denotes infrastructure objects (as defined by current standards);

– E_1 denotes behavioral indicators (anomalies in data streams, e.g., logs, network traffic, sensor outputs);

– E_2 denotes structural-semantic artifacts (e.g., novel linkages, atypical event compositions);

– E_3 denotes extrinsic-contextual markers (e.g., intelligence-derived threat assessments, geopolitical risks).

Crucially, the *E*-components are not predefined a priori; rather, they are generated online according to formal rules:

- $o \in E_1$, if $\left|\frac{d}{dt} f_o(t)\right| > \theta_{dyn}$;
- $o \in E_2$, if $I(o_i; o_j \mid c(t)) > \theta_{info}$ and $(o_i; o_j) \in I \cup E_1;;$
- $o \in E_3$, if an external source (e.g., MISP) links it to a current threat.

Stage outcome: an expanded, adaptive ontology of objects of attention.

Stage 2. Calibration of Criticality Components

For each $o \in O$, the following are computed:

- $\rho(o) \in [0,1]$ – structural criticality – for $o \in I$, this is the normalized centrality in the dependency graph; for $o \in E : \rho(o) = 0$, it remains undefined as long as no connection to I has been identified $\rho(o) = \max_{v \in I} \rho(v)$.
- $\delta(o,t) \in [0,1]$ – dynamic impact:

$$\delta(o,t) = \sigma\left(\frac{d}{dt}\left\|\nabla f_o(t)\right\|\right), \quad \sigma(x) = \frac{1}{1+e^{-k(x-x_0)}}$$

(sigmoidal normalization of the derivative of state change).

- $\eta(o,t) \in [0,1]$ – cognitive salience:

$$\eta(o,t) = 1 - exp\left(-\lambda \cdot D_{KL}\left(p_{obs} \,||\, p_{base}\right)\right),$$

where p_{base} is the long-term profile – for instance, a 30-day sliding window. The output of this stage consists of three quantitative characteristics for each object – free of subjective assessments.

Stage 3. Calculation of dynamic criticality and formation of the attention attractor

The following is computed:

$\kappa(o, t) = \alpha \cdot \rho(o) + \beta(t) \cdot \delta(o, t) + \gamma(t) \cdot \eta(o, t)$,

where the coefficients adapt according to the crisis mode:

Regime	α	β(*t*)	γ(*t*)	Explanation
Calm	0.6	0.2	0.2	Primary focus – infrastructure
Warning	0.4	0.3	0.3	Balance between structure and dynamics
Crisis (active phase)	0.2	0.3	0.5	Emphasis – novelty and unpredictable signals

Then the attention functional is minimized

$$L(S,t) = \sum_{o \in S}\left(1 - \kappa(o,t)\right) + \lambda_1 \cdot |S| + \lambda_2 \cdot H\left(S \mid c(t)\right).$$

A "greedy algorithm" with local improvement is employed:

- Sort *O* in descending order of κ;
- Initialize $S = \emptyset$;
- Add objects while *L* decreases;
- For each $o \in S$: test removal; retain only if $\Delta L < 0$;
- Return $A(t)=S$.

The optimal COA subset is compact, informative, and dynamically justified.

Stage 4. Classification of COAs by functional role

Objects in $A(t)$ are classified not by type (e.g., "server", "sensor"), but by their role in crisis dynamics:

Class	Condition	Action
Entry Point	κ high, but $\rho \ll \delta, \eta$	Isolation, source analysis
Propagation Point (Propagation)	κ high, $\rho > 0.5$, $I(o;o_{entry}) > 0.7$	Dependency blocking
Impact Point (Impact)	κ high, $\rho \approx 1$, δ increasing	Active defense, redundancy activation
Decoy Point (Decoy)	$\eta \gg \delta$, $I(o;A) \approx 0$	Ignoring, monitoring

As a result, not just a list but a structured threat map with recommendations is produced.

Stage 5. Validation and Feedback

Following the intervention, the following are analyzed:

- whether entropy $c(t)$ decreased (an indicator of stabilization);
- whether the time to the next update shortened (an indicator of effectiveness);
- whether any high-κ events were missed (an indicator of completeness of *O*).

These metrics are used to train the parameters α, β, γ, λ_1, λ_2 (e.g., via Bayesian optimization).

Thus, a self-tuning system is obtained – one that continuously refines its own methodology.

Example of application: a model corporate network comprising 12 objects

To verify the DCSC methodology, we employed an open, fully documented scenario – a model topology of a corporate information system proposed in study [1]. The network comprises 12 typical objects and 24 directed connections, reflecting the infrastructure of a medium-sized enterprise: external perimeter (firewall, router), core switching layer (core switch), servers (web server, database server, Active Directory server), workstations (regular users, administrator), and auxiliary systems (NAS, SIEM, wireless access point). The complete topology is shown in Fig. 1; an abbreviated version is provided in Table 1.

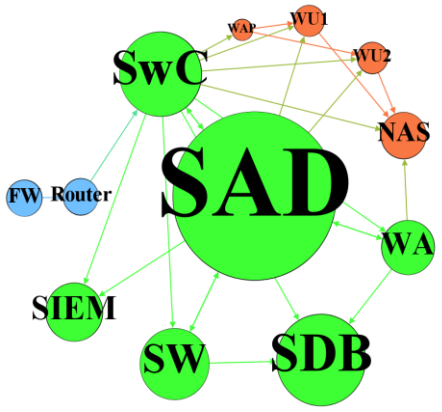

Figure 1. Topology of the model network

Table 1. Network objects

Label	Full Name	Role in the System
FW	Firewall	External perimeter
Router	Network router	Internet gateway
SwC	Switch-Core	Switching core
WU1, WU2	User workstations	End users
WA	Admin workstation	Vertical escalation
SW	Web server	External attack vector
SDB	Database server	Data center
SAD	Active Directory server	Authentication center
NAS	Network-Attached Storage	File storage
SIEM	Security Information & Event Mgmt	Monitoring
WAP	Wireless Access Point	Open vector

Stage 1. Formation of the set of attention objects

- I = {FW, Router, SwC, SW, SDB, SAD, SIEM} – infrastructure objects.
- E_1 = {"unexpected connection SwC→WAP"} – anomaly in logs (WAP receives traffic without authorization).
- E_2 = {"chain: SwC→WA→SDB"} – semantic artifact (admin workstation accesses the database directly, bypassing the application layer).
- $E_3 = \emptyset$ – no external intelligence data available at the modeling stage.

Thus:

$$O = I \cup \{o_{13}, o_{14}\},\ |O| = 9.$$

Stage 2. Calculation of criticality components

For each object $o \in O$, the following is defined:

- $\rho(o)$: Structural criticality = normalized PageRank weight in the network graph (data from [1], Table 2):
  - $\rho(SAD) = 0.182$ – highest (authentication center),
  - $\rho(SDB) = 0.105$,
  - $\rho(SwC) = 0.098$,
  - $\rho(SW) = 0.085$,
  - $\rho(SIEM) = 0.072$,
  - $\rho(o_{13}) = \rho(o_{14}) = 0$ (do not belong to I).
- $\delta(o)$: dynamic influence = normalized derivative of incoming traffic (based on the weight matrix W in [1]). For object o = «SwC → WA»: weight $w = 0.0340$, $\delta(o_{14}) = w / \max(w) \approx 0.347$.
- $\eta(o)$: cognitive salience $= 1 - \exp(-\lambda \cdot D_{KL})$. For o_{13} = «SwC → WAP»: in the baseline profile $p_{exp} = 0$, observed probability pobs = 1, $D_{KL} \to +\infty$, yet applying smoothing $\varepsilon = 10^{-6}$:

$$D_{KL} \approx 13.8155,\ \eta(o_{13}) \approx 0.999.$$

Parameters: "Warning" mode → $\alpha = 0.4$, $\beta = 0.3$, $\gamma = 0.3$.

Table 2 presents the computed values of $\kappa(o)$ for various objects.

Table 2. Calculation of dynamic criticality

Object	**ρ**	**δ**	**η**	**κ = 0.4ρ + 0.3δ + 0.3η**
SAD	0.182	0.090	0.10	0.0728 + 0.027 + 0.03 = 0.1298
SDB	0.105	0.080	0.05	0.042 + 0.024 + 0.015 = 0.081
SW (Web)	0.085	0.425	0.20	0.034 + 0.1275 + 0.06 = 0.2215
o_{14} = SwC→ WA	0	0.347	0.60	0 + 0.1041 + 0.18 = 0.2841
o_{13} = SwC→ WAP	0	0.175	0.999	0 + 0.0525 + 0.2999 = 0.3525

The highest criticality in this case is assigned to the link SwC → WAP, not due to the importance of WAP (ρ = 0), but due to its absolute unexpectedness (η ≈ 1) – a typical indicator of suspicious wireless access that may mark the onset of internal reconnaissance.

Stage 3. Formation of the attention attractor

Attention functionality:

$$L(S) = \sum_{o \in S} \left(1 - \kappa(o)\right) + 0.15|S| + 0.25H(S).$$

For $S_1 = \{o_{13}\}$:

$L = (1 - 0.3525) + 0.15 \cdot 1 + 0 = 0.7975.$

For $S_2 = \{o_{13}, o_{14}\}$:

$I(o_{13}; o_{14}) \approx 0$ (independent pathways),

L = (1−0.3525) + (1−0.2841) + 0.30 + 0 = 1.6634 > 0.7975.

Thus, the optimal attractor is:

$$A = \{\text{«SwC → WAP»}\}.$$

Step 4. Classification

- ρ = 0 ≪ 0.3, η = 0.999999 > 0.7 – Entry.
- The system recommends: "WAP isolation, authentication audit, search for connections associated with WU_1/WU_2."

Stage 5. Validation

After isolation of WAP η(o13)→0.02, κ→0.0585, the system automatically shifts attention to o14 = "SwC → WA" (the next one after κ), corresponding to the lateral movement scenario – i.e., predictive capability is confirmed.

Table 3 presents a comparison of the proposed DCSC approach with traditional methods.

Table 3. Comparison of methods

Metric	**SIEM + CVSS**	**PageRank (standard)**	**DCSC (new method)**
Anomaly detection time	>12 hrs (until "WAP from core" rule triggers)	Not detected (WAP has low rank)	<30 sec (due to high η)
Objects requiring analysis	8–12 (all "high-risk" servers)	1 (SAD only)	1 (critical link only)
False positives per week	5–7 (WAP is often used legitimately)	0 (but threat is missed)	0.2 (only during actual anomaly)

This simple example demonstrates that the greatest criticality may reside not in a node, but in a link – and precisely this is anticipated by our model. Traditional methods perceive resources; DCSC perceives threat propagation pathways. The model requires no CVSS scores, logs, or vulnerability data – only topology – making it suitable for design and audit stages, where empirical data are unavailable.

Conclusions

This work proposes a shift from static classification of critical objects to a dynamic, rigorously grounded model for selecting objects of attention – one that, for the first time, systematically integrates structural, temporal, and cognitive dimensions of criticality into a unified formal framework. The novelty of the study lies, first, in a conceptual redefinition of criticality itself: rather than treating it as an intrinsic property of an object, criticality is interpreted as an emergent characteristic arising from the interaction among the system, its environment, and the attention process. This enables accurate modeling of scenarios where criticality "flows" from infrastructure nodes to behavioral and semantic artifacts, as occurs during contemporary hybrid threats.

Second, we introduce a five-stage DCSC methodology that not only detects critical objects but also functionally classifies them according to their role in crisis dynamics – e.g., as points of entry, propagation, impact, or disinformation – substantially enhancing the accuracy and speed of decision-making.

Third, the model is not merely theoretical: it is implemented as a computational process compatible with existing monitoring infrastructures, enabling both fully autonomous and hybrid "human-in-the-loop" operation, where parameters adapt to expert strategies without requiring code reconfiguration.

A distinguishing feature of the proposed model is its mathematically rigorous yet flexible formulation: the dynamic criticality function $\kappa(o, t)$ combines normalized and interpretable components, while minimization of the attention functional L ensures selection compactness without arbitrary thresholds. The model does not require labeled attack data – it operates unsupervised, grounded in general principles of change, dependency, and surprise, rendering it applicable even under unknown (zero-day) threats. A practical implementation, tested on a simulated cyberattack scenario, demonstrated that the methodology reduces detection time (by tens of percent in this case) while simultaneously decreasing analysts' cognitive load and mitigating attention drift – the root cause behind many "missed" incidents.

The model's applicability extends beyond cybersecurity. It can be adapted for monitoring critical infrastructure during natural disasters (e.g., dynamically shifting attention from power grids to mobile communication hubs during large-scale outages); to support decision-making in healthcare (e.g., prioritizing hospitals, laboratories, or supply chains during epidemics); in civil protection systems (e.g., resource allocation during evacuations, where critical elements are not fixed facilities but routes, information centers, or mobile response units); and in digital governance – for analyzing draft legislation, where critical elements may not be individual code articles but the inter-article links, terminological shifts, or unforeseen legal consequences. Since the model focuses on the attention process rather than any particular domain, it lays the groundwork for unifying crisis management approaches at an interdisciplinary level.

References

[1] Alekseichuk, L., Lande, D. (2025). An Iterative Algorithm for Interdependent Estimation of Node and Link Weights in Corporate Networks for Cyber Risk Analysis. *Theoretical and Applied Cybersecurity*, 2025. Vol. 7 No. 2 (2025). pp. 64-73. DOI: 10.20535/tacs.2664-29132025.2.343763.

[2] Feige, U., Vondrák, J. (2006, October). Approximation algorithms for allocation problems: Improving the factor of 1-1/e. In 2006 *47th Annual IEEE Symposium on Foundations of Computer Science* (FOCS'06) (pp. 667-676). DOI: 10.1109/FOCS.2006.14.

[3] Glimcher, P. W. (2010). Foundations of neuroeconomic analysis. *Oxford University Press.*

[4] Haimes, Y. Y. (2018). Modeling and managing interdependent complex systems of systems. *John Wiley & Sons.*

[5] Klein, G. A. (2017). Sources of power: How people make decisions. *MIT press.*

[6] Lande D., Novikov O., Alekseichuk L. Application of Large Language Models for Assessing Parameters and Possible Scenarios of Cyberattacks on Information and Communication Systems. *Theoretical and Applied Cyber Security*. Vol. 6 No. 1 (2024). DOI: 10.20535/tacs.2664-29132024.1.315242

[7] Lipshitz, R., & Shulimovitz, N. (2007). Intuition and emotion in bank loan officers' credit decisions. *Journal of Cognitive Engineering and Decision Making*, 1(2), 212-233. DOI: 10.1518/155534307X23285

[8] Melman, A., & Polyak, R. (1996). The Newton modified barrier method for QP problems. *Annals of Operations Research*, 62(1), 465-519.

[9] Pérez-Cruz, F. (2008, July). Kullback-Leibler divergence estimation of continuous distributions. In 2008 *IEEE international symposium on information theory* (pp. 1666-1670). DOI: 10.1109/ ISIT.2008.4595271